Executive Summary and Technical Recommendation:

The Encryption Subcommittee has convened regularly since August of 2017. In this time, the Subcommittee has assessed the need for encrypted interoperable talk groups and explored the technical issues with an encrypted interoperable environment. Given this acquired information and set of conclusions, the Encryption Subcommittee submits a technical recommendation to ISICSB that users of the ISICS Platform who have a desire to utilize secure, encrypted interoperable talk groups available in the ISICS Regional Interoperable and Statewide Talk Groups Fleet Map purchase multi key subscriber units.

The Encryption Subcommittee recommends that the encrypted interoperable talk groups specified in the Detailed Design Review (DDR) be left in the programming code plug for user groups. However, encrypted interoperable talk groups should remain inactive until encryption is deployed and tested on the ISICS Platform. This includes dissemination of traffic encryption keys (TEK) and dissemination and enactment of policies and procedures that affect encrypted interoperable communication along with associated costs.

The Encryption Subcommittee also recommends designations be made for suggested use of some interoperable talk groups.

These recommendations apply to the specified encrypted interoperable talk groups on the ISICS fleet map. This does not apply to local geopolitical operable talk groups.

These recommendations do not apply to a local agency or entity that may want to utilize vendor-specific encryption algorithms and schemes or Data Encryption Standard (DES) variants for local operability.

Summary of Proceedings:

The current land mobile radio (LMR) landscape in Iowa consists of several district networks that are often oriented around geopolitical boundaries or subdivisions. The vast majority of these networks operate in the conventional VHF spectrum. Primary interoperable communications pathways in the past have been done without encryption (in the clear).

The buildout of the P25 Phase II trunked Iowa Statewide Interoperable Communications System (ISICS) Platform presents several new opportunities for interoperable communications that did not previously exist in Iowa. In addition to statewide coverage and more user capacity, one of these new features is encryption on interoperable talk groups.

Up to three encrypted interoperable talk groups were allocated for each region and statewide for a total of 21 encrypted interoperable talk groups during the detailed design review (DDR) in 2015. The preferred method of encryption was to be AES256.

The Encryption Subcommittee convened for the first time in August 2017 to explore encrypted interoperable talk groups on the ISICS Platform and develop recommendations and policies for encrypted interoperable talk groups on ISICS. The Subcommittee is comprised of representatives from a local municipal dispatch center, State of Iowa Radio Dispatch, State of Iowa technicians, local sheriff's office representatives, federal law enforcement, local municipal police and fire, state university police, emergency management, Iowa State Patrol, Iowa Department of Criminal Investigation and statewide interoperability coordinator.

In the first meeting, a desire for secure communication was conveyed among the various user group representatives. Several scenarios where identified in which encrypted interoperable channels would benefit multi-agency and/or multijurisdictional communications during planned and unplanned events.

In addition, it was recognized that federal agencies are obligated to be compliant with Federal Information Security Management Act of 2002 (FISMA) in their own communications and when operating on other networks. This includes adherence to National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) when and where they apply. This means federal agencies must utilize AES256 encryption in their operable and interoperable communications when LMR traffic is sensitive but unclassified. This includes communication with state and/or local agencies. Utilizing AES256 encryption would allow for various federal agencies to securely communicate with state and/or local agencies.

In subsequent meetings, the Encryption Subcommittee has recognized there are limitations with how subscriber radios can communicate under an encrypted environment. Technical difficulties exist regarding key management as well. These limitations stem from several sources, but work is on-going within TIA/TR-8.3 (standards-setting committee) to enhance pathways for encrypted interoperable communications and key management. Manufacturers have worked to mitigate technical challenges that affect the ability to securely communicate between single key and multi key subscriber units.

The Encryption Subcommittee met on November 28, 2017 met with representatives from TR-8.3 to discuss the current status of several standards, on-going development of those standards and items that are for future study. The TR-8.3 members represented Harris, Motorola, EF Johnson, Federal Bureau of Investigation (FBI), Department of Homeland Security Office of Emergency Communication (OEC) and Federal Partnership for Interoperable Communications (FPIC).

During the meetings, the following conclusions were reached:

- Interest in encrypted LMR capability is increasing and expanding;
- There are advantages and disadvantages inherent to single key and multi key subscriber units;
- EF Johnson, Harris and Motorola subscriber units' software has been updated to allow for a complete range of key IDs (KIDs) to be assigned to a traffic encryption key (TEK);
- Multi key subscriber units offer the most flexibility for a diverse array of users, allow for separate TEKs for operability but present management challenges;
- Single key subscriber units represent the most basic goal of encryption by eliminating scanner eavesdropping but may limit interoperability;
- An agency that desires to flash update subscriber units to multi key encryption (if possible) may have to allocate significantly more funds to for those updates when compared to purchasing a multi key radio at the time of initial procurement;
- An agency or geopolitical subdivision that purchases a single key radio may need to use the statewide key in order to interoperate with other agencies in addition to local operability;
- FPIC has a standing recommendation that agencies utilize the capability and flexibility offered by multi key AES256 equipped radios;
- Efforts should be made at a state level to keep the number of TEKs utilized on the ISICS Platform to a minimum to maintain consistency with the DDR;

- There may be agencies in Iowa that possess subscriber units that do not currently offer encryption or may have purchased single key radios;
- Coordination with other agencies and entities will need to occur to ensure interoperability exists;
- Encrypted interoperable talk groups need to be optional on the ISICS platform, and not every user will need access to them;
- The current set of encrypted interoperable talk groups may need to remain inactive until set policies and procedures for usage are defined;

Given this acquired information and set of conclusions, the Encryption Subcommittee submits a technical recommendation to ISICSB that users of the ISICS Platform who have a desire to utilize secure, encrypted interoperable talk groups available in the ISICS Regional Interoperable and Statewide Talk Groups Fleet Map purchase multi key subscriber units.

The Encryption Subcommittee recommends that the encrypted interoperable talk groups specified in the DDR be left in the programming code plug for user groups. However, encrypted interoperable talk groups should remain inactive until encryption is deployed and tested on the ISICS Platform. This includes dissemination of TEKs and dissemination and enactment of policies and procedures that affect encrypted interoperable communication along with associated costs.

The Encryption Subcommittee also recommends designations be made for suggested use of some interoperable talk groups.

These recommendations apply to the specified encrypted interoperable talk groups on the ISICS fleet map. This does not apply to local geopolitical operable talk groups.

These recommendations do not apply to a local agency or entity that may want to utilize vendor-specific encryption algorithms and schemes or DES variants for local operability.